Rialtas na hÉireann
Government of Ireland

Trust or Company Service Providers Risk Assessment

Update of Ireland's National AML/CFT Risk Assessment

Table of Contents

Acronyms

4AMLD	EU 4th Anti-Money Laundering Directive
5AMLD	EU 5th Anti-Money Laundering Directive
AGS	An Garda Síochána
AML	Anti-Money Laundering
AMLCU	Anti-Money Laundering Compliance Unit, Department of Justice
AMLSC	Anti-Money Laundering Steering Committee
BO	Beneficial Ownership
CBI	Central Bank of Ireland
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CJA 2010	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended
CLO	Collateralised Loan Obligation
CSR	Country Specific Recommendation
DAB	Designated Accountancy Body
EC	European Commission
EEA	European Economic Area
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ICAV	Irish Collective Asset-management Vehicle
ML	Money-Laundering
MoU	Memorandum of Understanding
NRA	National Risk Assessment
PEP	Politically Exposed Person
RBO	Register of Beneficial Ownership
SNRA	EU Supranational Risk Assessment
SPV	Special Purpose Vehicle
STR	Suspicious Transaction Report
TCSP	Trust or Company Service Provider
TF	Terrorist Financing

1. Introduction

This report updates and replaces the section of Ireland's Money Laundering/Terrorist Financing (ML/TF) National Risk Assessment (NRA) (2019[1]) which considered the ML/TF risks of Trust or Company Service Providers (TCSPs).

It is part of Ireland's ongoing obligations under Article 7 of the 4th Anti-Money Laundering Directive (4AMLD) to take, "*appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it and [...] keep that risk assessment up to date.*"[2] Ireland is also obliged under FATF Recommendation 1 to *"take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country on an ongoing basis."*[3]

The sectoral risk assessment of TCSPs also forms part of a broader cross-governmental response to address the 2020 Country Specific Recommendations (CSR) (ST 8178/20 - COM(2020) 507 final) assigned to Ireland as part of the European Commission's European Semester process. The CSR[4] found that *"Ireland still faces [ML/TF] risks due to its internationally oriented economy, involving significant inflow of foreign direct investments, and the presence of complex legal structures with foreign sponsors. […] Inadequate understanding of risk exposure by these professionals results in a low reporting of suspicious transactions. The intensity of supervision is inadequate to remedy these issues and does not rest on a risk-based approach."* To address this issue, the CSR calls for Ireland to *"Ensure effective supervision and enforcement of the anti-money laundering framework as regards professionals providing trust and company services."*[5]

1.1 Definition and Overview

Trust or Company Service Providers (TCSPs) are defined by Section 24 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended (hereafter the 'CJA 2010 as amended').[6]

[1] Available at: 80ab9a41b1354405adcec66bfb1c0715.pdf (assets.gov.ie)

[2] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015L0849-20180709

[3] Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation,' available at: https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[4] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1591720698631&uri=CELEX%3A52020DC0507

[5] Council Recommendation available at : https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1591720698631&uri=CELEX%3A52020DC0507

[6] Consolidated legislation available at: https://revisedacts.lawreform.ie/eli/2010/act/6/front/revised/en/html

TCSPs are defined as "any person whose business it is to provide any of the following services:

(a) forming companies or other bodies corporate;

(b) acting as a director or secretary of a company under an arrangement with a person other than the company;

(c) arranging for another person to act as a director or secretary of a company;

(d) acting, or arranging for a person to act, as a partner of a partnership;

(e) providing a registered office, business address, correspondence or administrative address or other related services for a body corporate or partnership;

(f) acting, or arranging for another person to act, as a trustee of a trust;

(g) acting, or arranging for another person to act, as a nominee shareholder for a person other than a company whose securities are listed on a regulated market."

A TCSP is not prevented from providing other services in addition to the above, but once it does carry out any of the services referred to in the definition, it is a TCSP for the purposes of the CJA 2010 as amended. Under Section 25(1)(e) of the CJA 2010 as amended, a TCSP is "a designated person"[7] and as such it is subject to the obligations and requirements under the Act.

A designated person is subject to supervision and monitoring by a competent authority which is in turn defined in section 60. The supervision of TCSPs for AML/CFT purposes in Ireland is undertaken by a number of different competent authorities, depending on the nature of the TCSP. Section 61 of the CJA 2010 as amended provides that where there is more than one competent authority for a designated person under Section 60, those competent authorities may agree that one of them with act as the competent authority for that person.

In this regard, the relevant supervisors[8] of TCSPs are as follows:

1. The Central Bank of Ireland supervises TCSPs that are subsidiaries of regulated credit or financial institutions.

2. The Designated Accountancy Bodies (DABs)[9] - five prescribed accountancy bodies in Ireland act as competent authorities for their members under Section 60 of the CJA 2010 as amended and are responsible in specified circumstances for supervising members that provide TCSP services. A Memorandum of Understanding (MoU) between the DABs and the AMLCU of the Department of Justice governs this.[10] Table 1 contains information about the relevant competent authority in a given scenario. In three scenarios, the DAB is the competent authority and in two others, it is the Anti-Money Laundering Compliance Unit (AMLCU) of the Department of Justice.

[7] Irish legislation uses the term "designated persons," which should be considered synonymous with "obliged entities."

[8] The term "supervisor" should be considered synonymous with "competent authority" in this report.

[9] There were eight Designated Accountancy Bodies in Ireland at the beginning of this assessment. Two withdrew during the course of 2021. There are six at time of publication, but only five supervise TCSPs.

[10] Available at: https://www.amlcompliance.ie/wp-content/uploads/2019/11/AMLCU-MOU-with-Accountancy-Bodies.pdf

3. The AMLCU of the Department of Justice supervises any remaining TCSPs that do not fall to be supervised by either the Central Bank or a DAB. Under the CJA 2010 as amended, the Minister for Justice is the competent authority by default, where there is no other competent authority specified for a particular category of designated persons. Under section 108 of the CJA 2010 as amended, the Minister for Justice has delegated the Minister's competent authority functions to the Principal Officer and Assistant Principal Officers in the AMLCU.

There is also a MoU outlining the position agreed between the Law Society and the AMLCU with regard to solicitors.[11] Under the MoU, the Law Society, as the competent authority for solicitors under the CJA 2010 as amended, has responsibility to monitor solicitors when they provide trust and company legal services and to take measures that are reasonably necessary for the purpose of securing compliance by solicitors with Part 4 of the CJA 2010 as amended. However, the MoU provides that when solicitors operate TCSPs through limited companies, the AMLCU is the competent authority. The TSCPs in such situations are corporate bodies separate from individual solicitors but which may be controlled by them, or in which they may participate. Because of the separate legal personality, a solicitor can (at a remove) provide the services of a TCSP and, as such, must be authorised by the Minister.

Table 1: MoU between the AMLCU and the DABs on the relevant competent authority

	TCSP Composition	Regulatory Responsibility	TCSP Obligation
1	Every Principal is a member of a particular Designated Accountancy Body (DAB).	The DAB is the competent authority for the TCSP.	To ensure it is subject to supervision by that DAB.
2	Every Principal is a member of a DAB, but every Principal is not a member of the same DAB.	Where there is more than one Principal and those Principals are members of different DABs, those DABs shall agree between them which of them will be the competent authority.	To ensure it is subject to supervision by appropriate DAB, as determined by reference to the principles set out in the Appendix to the MoU.
3	Where greater than 75% of the shares or voting rights are owned or controlled by members of DABs providing every Principal is a member of a DAB.	The DAB is the competent authority for the TCSP or where there is more than one Principal and those Principals are members of different DABs, those DABs will agree between them which of them will be	To ensure it is subject to supervision by that DAB, or to ensure it is subject to supervision by the appropriate DAB, as determined by reference to the principles set out in the Appendix to the MoU.

[11] Available at: https://www.amlcompliance.ie/wp-content/uploads/2019/11/AMLCU-MOU-with-Law-Society.pdf

	TCSP Composition	Regulatory Responsibility	TCSP Obligation
		responsible for monitoring the TCSP.	
4	One or more Principal(s) is not a member of a DAB.	The Minister (AMLCU) is the competent authority.	To ensure it is authorised by the AMLCU.
5	Every Principal is a member of a DAB, however, 25% or greater of the shares or voting rights are owned or controlled otherwise than by members of a DAB.	The Minister (AMLCU) is the competent authority.	To ensure it is authorised by the AMLCU.

The number of TCSPs operating in Ireland as of July 2021[12] is set out in Table 2.

Table 2: Number of TCSPs supervised by each competent authority as of July 2021

Supervisor	Number
Central Bank of Ireland (CBI)	33
Designated Accountancy Bodies (DABs)	388
Anti-Money Laundering Compliance Unit (AMLCU)	356
Total	**777**

Based on the questionnaire responses, the most common TCSP service provided by TCSPs operating in Ireland is *providing a registered office, business address, correspondence or administrative address or other related services for a body corporate or partnership,*" with 29.5% of TCSPs providing this service. This is followed by "*forming companies or other bodies corporate*," at 24.5%. Table 3 below sets out the reported number of TCSPs providing each TCSP service in Ireland.

[12] Based on the response to the questionnaire issued to TCSP competent authorities.

Table 3: Number of TCSPs providing each TCSP service under CJA 2010 as amended[13]

Category	Number
(a) forming companies or other bodies corporate;	190
(b) acting as a director or secretary of a company under an arrangement with a person other than the company;	154
(c) arranging for another person to act as a director or secretary of a company;	126
(d) acting, or arranging for a person to act, as a partner of a partnership;	43
(e) providing a registered office, business address, correspondence or administrative address or other related services for a body corporate or partnership;	229
(f) acting, or arranging for another person to act, as a trustee of a trust;	101
(g) acting, or arranging for another person to act, as a nominee shareholder for a person other than a company whose securities are listed on a regulated market.	96

1.2 Methodology

This Risk Assessment was prepared by a subcommittee of the Anti-Money Laundering Steering Committee, chaired by the Department of Finance. The report was drafted on the basis of both quantitative data and qualitative information received from each of the TCSP supervisors by way of a questionnaire, while drawing from the EU Supranational Risk Assessment and relevant Financial Action Task Force guidance. Unless otherwise indicated, information in the assessment below is based on the questionnaire responses.

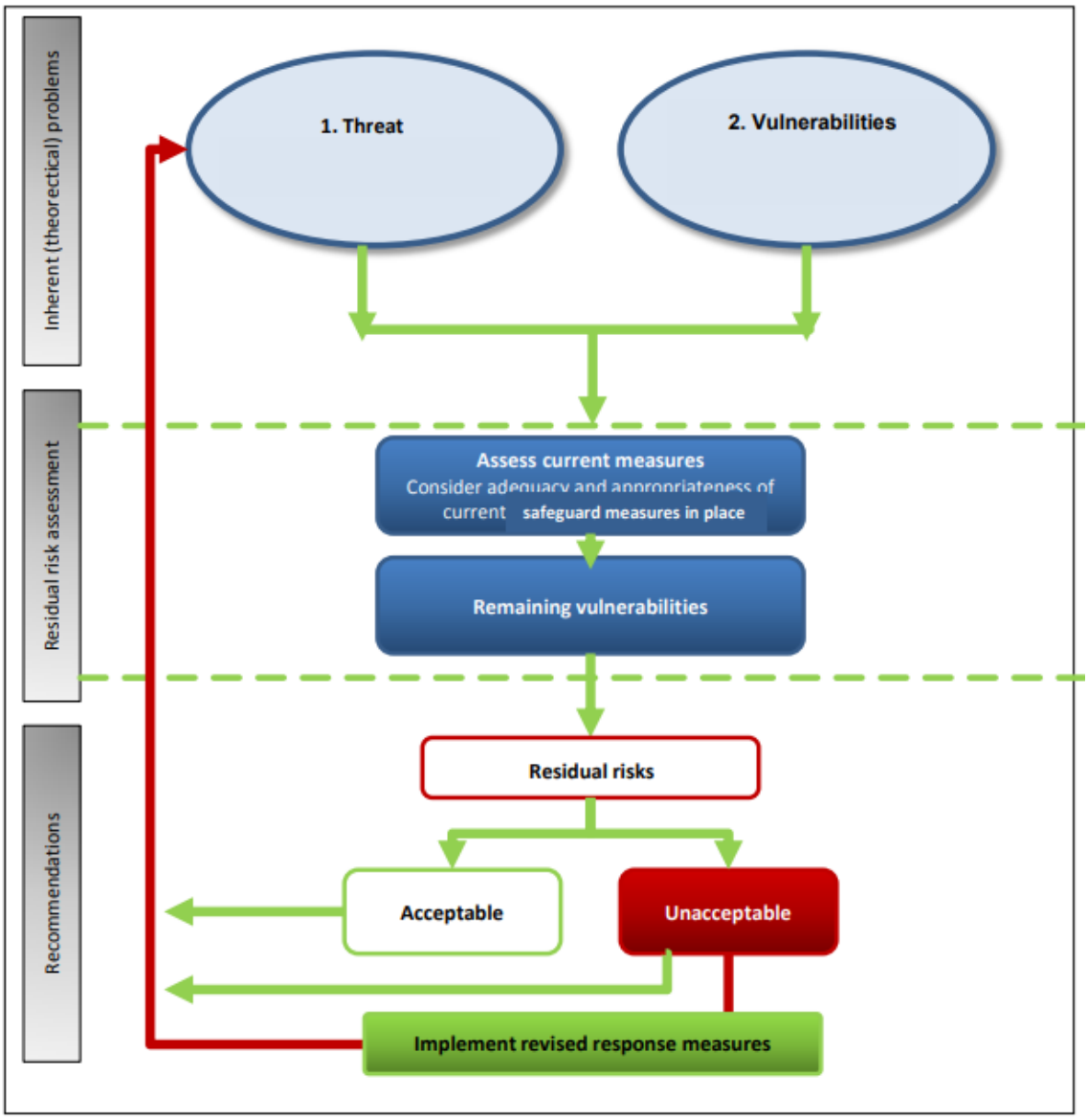
The Methodology applied in this assessment is the methodology recommended by the European Commission (EC), as applied in the EC's supra-national risk assessment (SNRA). An outline of the European Commission's Supranational Risk Assessment methodology can be found in the following document: "DG migration and home affairs and DG Justice and Consumers *Methodology for assessing the risk of money laundering and terrorist financing affecting the internal market and related to cross-border activities"*[14]. The EC explains that the conceptual framework can be summarised in the figure below.

[13] The total number is greater than the number of TCSPs as some provide more than one service.

[14] Available at: https://fatfplatform.org/assets/04112015-Methodology-SNRA-Clean-v1.1.pdf

Figure 1: Conceptual Framework underpinning the EU SNRA[15]

The conceptual framework for this methodology can be summarised as follows:



In the first step in the methodology, inherent problems are examined, which includes inherent threats and inherent vulnerabilities. The Commission has provided descriptors as follows:

[15] https://fatfplatform.org/assets/04112015-Methodology-SNRA-Clean-v1.1.pdf

Table 4: Rating of inherent Money Laundering /Terrorist Financing risks according to a four scale threat level

LOWLY SIGNIFICANT (value: 1)	No indicators that criminals have the intention to exploit this modus operandi for ML/TF. The modus operandi is extremely difficult to access and/or may cost more than other options and perceived as unattractive and/or highly insecure. No indicators that criminals have the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires more sophisticated planning, knowledge and/or higher technical expertise than other options. **The threat related to the use of this modus operandi is lowly significant.**
MODERATELY SIGNIFICANT (value: 2)	Criminals may have vague intentions to exploit this modus operandi for ML/TF. The modus operandi is difficult to access and/or may cost more than other options and be perceived as unattractive and/or insecure. Few indicators that criminals have some of the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires more planning, knowledge and/or higher technical expertise than other options. **The threat related to the use of this modus operandi is moderately significant.**
SIGNIFICANT (value: 3)	Criminals have exploited this modus operandi for ML/TF. The modus operandi is accessible and/or represents a financially viable option. The modus operandi is perceived as rather attractive and/or fairly secure. Criminals have the necessary capabilities to exploit this modus operandi. The modus operandi requires moderate levels of planning, knowledge and/or technical expertise. **The threat related to the use of this modus operandi is significant.**
VERY SIGNIFICANT (value: 4)	Criminals have recurrently exploited this modus operandi for ML/TF. The modus operandi is widely accessible and available via a number of means and/or relatively low cost. The modus operandi is perceived as attractive and/or secure. Criminals are known to have the necessary capabilities. The modus operandi is relatively easy to abuse, requires little planning, knowledge and/or technical expertise compared to other options. **The threat related to the use of this modus operandi is very significant.**

In the second step, remaining vulnerabilities, taking account of the existence and effectiveness of safeguards, are determined by assessing mitigating measures currently in place and considering what vulnerabilities remain once these are taken into account.

Table 5: Rating of remaining Money Laundering /Terrorist Financing vulnerabilities, taking account of the existence and effectiveness of safeguards, according to a four scale threat level

LOWLY SIGNIFICANT (value: 1)	[Within the sector/area considered, deterrence measures and controls exist and are effective at deterring money laundering and financing terrorism. The sector shows a positive organisational framework and a negligible exposure to the risk of ML/TF] **Illustrative assessment criteria:** **RISK EXPOSURE** - No or very limited products, services or transactions that facilitate speedy or anonymous transactions; secured and/or monitored delivery channels; low level of financial transactions; low level of cash based transactions; high quality management of new technologies and/or new payment methods. - Very limited volume of higher risk customers high ability to manage corporate entities or trusts in customer relationships. - No or very limited business and customer based in areas identified as high risk; low level of cross-border movements of funds. **AWARNESS OF THE RISK VULNERABILITY** Sector concerned shows a satisfactory level of awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from a positive organisational framework. - Competent authorities provide a comprehensive ML/TF risk assessment related to the sector and LEAs have a high ability to counter ML/TF risks (a range of ML/TF cases is visible and highly likely to be detected, leading to investigation, prosecution and convictions). - Good ability of the FIU to detect and analyse the risks, to ensure a good functioning of gathering information through STRs, in particular through the use of tailor-made indicators and a sufficient amount of resources to actually perform the risk-analysis. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework is commensurate to the risks inherent to this sector. - Controls [defined by the legislation] are effectively applied by the sector. Reliable CDD/identification mechanisms are in place to ensure adequate identification and verification process of a customer. Internal controls are applied by obliged entities in a robust manner (e.g. risk management, record keeping, training). Obliged entities are effectively reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a good level of sharing of information. **=> Lowly-significant vulnerabilities.**
MODERATELY SIGNIFICANT (value: 2)	[Within the sector/area considered, deterrence measures and controls exist and are reasonably effective at deterring money laundering and financing terrorism. The sector shows an organisational framework presenting some weaknesses and/or an exposure to the risk of ML/TF] **Illustrative assessment criteria**:

	RISK EXPOSURE - Limited products, services and transactions that facilitate speedy or anonymous transactions; mostly secured and/or monitored delivery channels; rather significant level of financial transactions; rather significant cash based transactions; good management of new technologies and/or new payment methods. - Few higher risk customers; good ability to manage corporate entities or trusts in customer relationships. - Some business and customer are based in areas identified as high risk; rather significant level of cross-border movements of funds. **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows some awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from an organisational framework, which shows some weaknesses. - Competent authorities provide a reasonable ML/TF risk assessment related to the sector and LEAs have a good ability to counter ML/TF risks (a range of ML/TF cases is visible and likely to be detected, leading to some investigations, prosecutions and convictions). - FIU can detect and analyse the risks in certain circumstances, to ensure a good functioning of gathering information through STRs, in particular through the use of tailor-made indicators. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework covers in major parts the risks inherent to this sector. - Controls [defined by the legislation] are applied by the sector but are presenting some weaknesses. Reliable CDD/identification mechanisms are in place but do not systematically ensure an adequate identification and verification process of a customer. Internal controls are applied by obliged entities to some extent (e.g. risk management, record keeping, training). Obliged entities are reporting few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a partial sharing of information. **=> moderately significant vulnerabilities**
SIGNIFICANT (value: 3)	[Within the sector/area considered, deterrence measures and controls have limited effects in deterring criminal/terrorist abuse of the service. The sector shows an organisational framework presenting very significant weaknesses and/or a significant exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **RISK EXPOSURE** - Significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; few secured and/or monitored delivery channels; significant level of financial transactions; significant cash based transactions; low management of new technologies and/ new payment methods.

	- Significant volumes of higher risk customers; low ability to manage corporate entities or trusts in customer relationships. - Major part of business and customer is based in areas identified as high risk; significant level of cross-border movements of funds. **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows limited awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, and training, allocated resources). The sector benefits from a limited organisational framework. - Competent authorities provide for a limited ML/TF risk assessment to the sector and LEAs have low capacity to counter ML/TF risks (only some ML/TF cases are visible and unlikely to be detected, leading to few investigations, prosecutions and convictions). - The FIU can detect and analyse the risks only in limited circumstances which allows only a limited functioning of gathering information through STRs. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework does not cover the most substantial parts of the risks inherent to this sector. - Controls applied by the sector present significant weaknesses. Few reliable CDD/identification mechanisms are in place and, where in place, do not allow an effective identification and verification process of a customer. Internal controls are applied by obliged entities with very significant weaknesses (e.g. risk management, record keeping, training). Obliged entities are reporting very few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allow few possibilities of sharing of information. => Significant vulnerabilities
VERY SIGNIFICANT (value: 4)	[Within the sector/area considered, there are extremely limited or no measures and controls in place, or they are not working as intended. The sector shows an organisational framework presenting highly significant weakness and/or a high exposure to the risk of ML/TF] **<u>Illustrative assessment criteria:</u>** **RISK EXPOSURE** - Very significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; no secured and/or monitored delivery channels; very significant level of financial transactions; very significant cash based transactions; no management of new technologies and/or new payment methods. - Very significant volumes of higher risk customers; no ability to manage corporate entities or trusts in customer relationships - Business and customer are based in areas identified as high risk; very significant level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows no awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector has no adequate organisational framework to address the ML/TF risks.

	- Competent authorities don't provide for any ML/TF risks assessment to the sector and LEAs have no ability to counter ML/TF risks (detection is very difficult and there are very few/no financial or other indicators of suspicious activity. The level of investigations, prosecutions and confiscations is extremely low). - The FIU can detect the risks in very limited circumstances or in no circumstances. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework does not cover the risks inherent to this sector. - Controls applied by the sector present very significant weaknesses. No reliable CDD/identification mechanisms are in place and the basic identification and verification requirement process of a customer is not fulfilled. Internal controls are not properly applied by obliged entities (e.g. risk management, record keeping, training). Obliged entities are not reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, does not exist or does not allow sharing of information. **=> very significant vulnerabilities**

Recommendations are then considered in terms of whether risks are acceptable or unacceptable and recommendations are made in the case of unacceptable risks, to implement revised response measures.

Overall ML/TF risk (known as the Residual ML/TF risk) is calculated using the following methodology:

For each category of TCSP, following assessment, a rating has been assigned relevant to its Inherent Risk, and Remaining Vulnerability. The ratings are consistent with the SNRA rating definitions as set out above, and each rating was assigned a value on a scale from 1 to 4:

- Lowly significant (value: 1)
- Moderately significant (value: 2)
- Significant (value: 3)
- Very significant (value: 4)

It is important to note that the ML and TF Remaining Vulnerability rating is determined following consideration of all mitigating factors. The SNRA methodology requires the remaining vulnerabilities component be given more weight when determining the overall risk level; in accordance with the SNRA methodology, a weighting of 40% for Inherent Risk (threats and vulnerabilities before mitigation) and 60% Remaining Vulnerability (vulnerability after mitigation measures has been applied).[16] The risk rating scale employed in the Commission's SNRA methodology is set out below.

[16] European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, See Annex 3 for SNRA methodology.

https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

Table 6: EU's supra-national risk assessment (SNRA) Rating scale

Inherent Risk (i.e. Threats and Vulnerabilities before mitigation)	**Very Significant**	2.2	2.8	3.4	4
	Significant	1.8	2.4	3	3.6
	Moderately Significant	1.4	2	2.6	3.2
	Lowly Significant	1	1.6	2.2	2.8
		Lowly Significant	**Moderately Significant**	**Significant**	**Very Significant**
	Remaining Vulnerabilities (i.e. taking account of the existence and effectiveness of safeguards)				

RISK	
1-1,5	Lowly signficant LOW
1,6-2,5	Moderately signifcant MEDIUM
2,6-3,5	Significant HIGH
3,5-4	Very significant VERY HIGH

National Risk Assessment (NRA) Rating scale

The rating scale set out in this assessment, while based on the Commission's SNRA methodology, uses slightly different language to ensure consistency with Ireland's NRA and other published sectoral risk assessments, undertaken prior to the development of the SNRA methodology.

Once a rating is calculated using the SNRA methodology, it is assigned a rating of low, medium-low, medium-high, or high as per Ireland's National Risk Assessment (NRA) rating.

Table 7: Equating the SNRA to the NRA scale

SNRA Rating Scale	NRA Rating Scale
Lowly significant (value: 1-1.5) LOW	Low
Moderately significant (value: 1.6-2.5) MEDIUM	Medium-Low
Significant (value: 2.6-3.5) HIGH	Medium-High
Very Significant – (value 3.5-4) VERY HIGH	High

2. Nature of Risks faced by TCSPs

The Financial Action Task Force (FATF) is the global standard-setter for AML/CFT policy. Among other functions, it regularly publishes guidance designed to support the implementation of the risk-based approach by policymakers, competent authorities and designated persons. In its "Guidance on applying the Risk-Based Approach to Trust and Company Service Providers,"[17] FATF notes that the functions and structure of TCSPs can vary greatly. They may provide a considerable range of services and activities, influenced by a varied client profile, as well as the size, focus, ownership profile and sophistication of the TCSP itself. In that context, FATF notes that TCSPs need to make reasonable judgements that reflect their particular services and activities.

Appropriate mitigation measures depend on the nature and risks arising from the TCSP's role and involvement in the affairs of its clients. Circumstances may vary considerably between TCSPs e.g. between those that represent clients directly as trustees or directors, controlling the affairs of the legal arrangement or legal person; and those that are engaged for distinct purposes such as only providing the service of registered offices and that have to rely on external directors for information on the client's activities.

FATF considers lack of transparency around beneficial ownership as the key risk pertaining to TCSPs, noting that *"criminals may seek the opportunity to retain control over criminally derived assets, while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and often trusts and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies, which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy."*[18]

FATF also assesses that criminals may also seek to misuse shelf companies formed by TCSPs, by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be with a view to creating the impression that the company is reputable and trading normally, having been in existence for many years. Shelf companies might also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

TCSPs may be involved in the formation, management, or administration of legal entities and arrangements. Where TCSPs play this "gatekeeper" role, they may find it challenging to obtain and keep current and accurate beneficial ownership information depending on the nature and activities of their clients. They may also face challenges when taking on new clients where there is minimal economic activity associated with the legal entity and/or its owners, controlling persons, or beneficial owners. There may also be specific challenges associated with taking on clients established in another jurisdiction.

FATF notes that even if the source of beneficial ownership information is available in a public registry, that does not guarantee the correctness of the information, in particular where the underlying information has been self-reported. Those risks notwithstanding, FATF notes that determining beneficial ownership should almost always start with questions to the immediate

[17] Financial Action Task Force (2019), *Guidance for a Risk-Based Approach to Trust and Company Service Providers*, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf

[18] FATF, *Guidance to TCSPs,* p.9.

client, having determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the client is a publicly listed company. The information provided by the client should then be appropriately confirmed by the TCSP by reference to public registers and other third party sources, where possible. This may require further questions to be put to the client. At the end of the onboarding of a client, the TCSP needs to be reasonably satisfied about the identity of the beneficial owner and should understand the nature of the business of the clients it is taking on.

FATF highlights that where a TCSP lacks sufficient expertise, understanding and knowledge of the risks faced, it may make flawed judgements. For example, TCSPs may overestimate risk, which could lead to wasteful use of resources, or they may underestimate risk and deploy insufficient resources, thereby creating vulnerabilities. FATF notes that competent authorities, including supervisors and self-regulating bodies should employ skilled personnel, who are technically equipped commensurate with the complexity of their responsibilities.

Analysis undertaken by the European Commission for the supranational AML/CFT risk assessment is consistent with FATF's in relation to how TCSPs may be misused and again highlights risks around lack of transparency of beneficial ownership. The Commission found[19] that criminals may seek to create complex structures involving many jurisdictions, in particular offshore jurisdictions with secretive chains of ownership, normally through shell companies,[20] where the owner of another company or another legal structure is registered elsewhere. Nominees are designated and will only appear to be in charge of the company by hiding the link with the true beneficial owner. By involving offshore companies, the perpetrators can stay anonymous, return the funds derived from criminal activity into the legal economy and commit tax fraud, tax evasion and other activities that impair the State budget or conceal the sources of the funds. This involves creating 'opaque structures', which are defined as structures where the true identity of the ultimate beneficial owner(s) of entities and arrangements in that structure is concealed, for example, through the use of nominee directors. In such cases, it is only the nominee director who appears to be the beneficial owner of the company.

2.1 Theoretical Examples of TCSP Misuse

Example 1: Illicit proceeds of crime are generated by criminals. The criminals ask a TCSP to set up a trust on their behalf and ask the TCSP to provide a trustee service. Illicitly generated funds are sent to the trust. The trust uses the funds to acquire shelf companies and to create a complex network of companies. The TCSP is asked to provide nominee shareholder services. Payments and transactions take place between the various companies. All of the companies' profits are received as profits by the trust. The TCSP as trustee then distributes the funds back to its client.

Example 2: The TCSP sets up a company for its client. The company established is a shell company. The TCSP is asked to provide nominee shareholder services to the shell company. The shell company is used to open a bank account. Criminals make payments from criminal proceeds to the bank account for fictitious services provided by the shell company.

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN

[20] An overview of shell companies in the European Union: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/627129/EPRS_STU(2018)627129_EN.pdf.

Example 3: One or a number of TCSPs are appointed as nominee directors of multiple legal entities across multiple jurisdictions. Third party advisors instruct the TCSPs to make transfers between the legal entities. Due to the layers created, the transactions are complex and permit the criminal to distance illicitly generated funds from their source.

3. Inherent Risks of TCSPs

This section considers the inherent risk of ML and TF posed by each TCSP service under the CJA 2010 as amended.

3.1 Inherent Risk of Money Laundering

3.1.1. (a) Forming companies or other bodies corporate

A TCSP may be asked by a client to establish a company or multiple companies, which the client could then use for criminal purposes. A TCSP faces risks of facilitating ML if it has not sought adequate information regarding the client on whose behalf it is setting up the company and if the TCSP is unclear about the purpose for which the company is intended to be used by the client. A TCSP may be exposed to misuse for criminal purposes if the ultimate beneficial owners of the legal entities being formed are unclear.

Company formation may be misused by perpetrators of ML/TF to create a veneer of legitimacy and to navigate the regulatory and reporting framework. Having a company established permits registration with the Companies Registration Office and makes it easier to open a bank account.

TCSPs may be asked by a client to transfer ownership of a company that was established by the TCSP some time ago but has no economic activity. The client could potentially misuse these so called “shelf companies” for criminal purposes as part of a network of companies, while creating the impression of operating an established business. A TCSP could be asked to set up a company on behalf of an offshore intermediary and to provide nominee director services, when it is unclear who is the ultimate beneficial owner of the company. For example, the ultimate owner could be based in a risky jurisdiction and the company could potentially be misused for fraudulent purposes.

3.1.2. (b) acting as a director or secretary of a company under an arrangement with a person other than the company

(c) arranging for another person to act as a director or secretary of a company

(d) acting, or arranging for a person to act, as a partner of a partnership.

The TCSP may be asked to provide these services on behalf of companies with non-Irish beneficial owners and where the jurisdiction is a risk factor in terms of the location of the beneficial owner. Even if not based in a high-risk jurisdiction, this service presents a higher risk of ML/TF due to the difficulty in verifying the beneficial owner and understanding the nuances of any relevant foreign law.

Risks include the client seeking to keep the identity of the actual owner, or of the controlling interests, confidential. A TCSP may be asked to act as company secretary or director to a non-Irish based entity or to a PEP. The inherent risks related to the geographic region and in providing the service to a PEP need to be considered. Acting as a director provides a veneer of legitimacy and assistance in navigating the regulatory and reporting company law framework, potentially sidestepping indicators that would have flagged possible criminality.

Nominee directors are generally appointed by companies, often due to an entity being from outside the EEA. While under the Companies Act 2014[21], the nominee director has the same obligations as any other director, it is imperative that the TCSP ensures it has a good knowledge of the company, its purpose and activity.

In providing these services, the TCSP acting as director or nominee director, or the director arranged for by the TCSP, becomes personally liable for any decisions or actions taken by the company and thus must ensure that it applies an appropriate level of control over actions and transactions. Furthermore, these services potentially enable awareness of all of the company's transactions and decisions, especially in cases where the director has a broad mandate. These may assist with limiting the risk of ML/TF.

The TCSP acting as the secretary of a company, or arranging for another person to act as the secretary of a company, presents a lower risk of ML/TF as that generally involves duties that have little to no connection to those typically carried out to launder illicit funds (such as investment or international wire transfers). However, there may be instances where secretaries can be misused and present higher risk of ML/TF, such as using administrative functions to create a veneer of legitimacy and to disguise criminal activity within a company.

A TCSP may be requested to act for multiple companies with common owners, where the beneficial owners may not wish their business relationships to be open to scrutiny. There may be a risk of the TCSP not understanding why it is being asked to provide these services. Furthermore, if requested to provide a company secretarial service to a non-Irish-based entity, there is a risk that the TCSP may not sufficiently assess the risks of providing such a service; including the risks associated with not having a locally-based company secretary, or risks related to the jurisdiction in which the entity is based.

These services are less risky where the TCSP is requested to provide director, secretary or other such services as an administrative tool until all legal requirements related to establishing a company are completed, or where the TCSP is asked to be a neutral party separating interested parties e.g. during a merger. It is also less risky when a TCSP is providing services to Public Limited Companies (PLCs).

The *Legal Persons and Legal Arrangements Risk Assessment*[22] found that the planning, knowledge and technical expertise required for ML/TF through a partnership, compared to other vehicles, acted as a mitigant to criminal misuse. However, this mitigant is nullified where a TCSP is providing a partnership, as they provide the relevant technical expertise. It was reported as part of the questionnaire that partnership services was the least frequently provided service by TCSPs in Ireland. However, the Companies Registration Office has noted that while the overall number of partnerships registered in Ireland remains modest[23] (less than 3,000 active), most of these have been registered since 2015, which indicates a trend towards the greater use of partnerships.

[21] Available at: https://revisedacts.lawreform.ie/eli/2014/act/38/revised/en/html

[22] Available at: https://assets.gov.ie/75052/d586a59d-2f1d-48b6-b1cc-857c9316cc42.pdf

[23] https://www.cro.ie/Publications/LTD-Partnerships

3.1.3. (e) providing a registered office, business address, correspondence or administrative address or other related services for a body corporate or partnership

Virtual office addresses may be used in investment frauds. Providing registered office services carries risks, particularly where there is little face-to-face engagement. Services such as the forwarding of large volumes of mail may provide the apparent comfort of an Irish nexus, while potentially obscuring the actual identity and location of recipient of the mail.

There are also risks where a TCSP is requested to provide multiple addresses to the same business or to offshore intermediaries. Multiple addresses could give the impression that a business is more substantial than it is, or could create an impression that it is a company with a local presence. If a TCSP supplies multiple addresses to the same or connected businesses, there is a risk that this service may be provided without a sufficient explanation or commercial basis from the client. The TCSP must ensure that it has sufficient information from the client before providing any such service.

Where a client is operated or owned by a non-Irish resident company or person, the appropriate level of due diligence in such circumstances needs to be considered carefully by the TCSP. The lack of in-depth scrutiny at on-boarding stage is an inherent risk if all the TCSP is doing for the client is providing registered address services as there is little opportunity to rectify misunderstandings between the TCSP and client or any other issues later on. Furthermore, due to the nature of this activity, there may be limited scope for the application of ongoing AML/CFT monitoring of the business activities of the client. A registered office or business address may also be used to open a bank account or access financial services, and could provide a business - with no nexus or connection to Ireland - with an explanation for transferring funds into the country.

The risk associated with registered office services is limited by:

- regular contact between the TCSP with the client;
- the physical collection of mail by client representatives;
- the TCSP providing a sole contact address for the client; and
- a client using the premises for board meetings or similar functions.

3.1.4. (f) acting, or arranging for another person to act, as a trustee of a trust

Providing trustee services may be misused to obscure beneficial ownership or the genuine purposes of the trust, with the riskiest scenario being where the source of the trust's funds are not clear and where the real beneficial owner is not named. This might include cases where a trustee has discretionary power to name a class of beneficiaries that does not include the real beneficiary or where a trust is set up with the intention of making it harder to determine the beneficiaries of assets managed by the trust, such as orphan structures.

Conversely, the source of funds being clear limits the risk significantly e.g. the risk associated with life assurance, share schemes and company pension funds is significantly lower.

There are also higher risks where the settlor, beneficiary or others have significant control over the assets and/or income of the trust. There is a risk from undue influence of the settlor or other third party over the trust, and Trustees must assess the extent to which they are free to act in the best interest of the beneficiaries. There is a risk that a TCSP acting as trustee may not have proper oversight of the assets of the trust to prevent bank accounts or other elements of the trust's administration framework being misused for unrelated purposes.

3.1.5. (g) acting, or arranging for another person to act, as a nominee shareholder for a person other than a company whose securities are listed on a regulated market

Nominee shareholder services provide confidentiality as to the actual owner or controlling interest of the company. Where a TCSP provides shareholder services for multiple companies with common owners, there is a risk that this service has been requested as the beneficial owners do not wish their business relationships to be scrutinised. This service also means the nominee shareholder, if a natural person, may appear on the Register for Beneficial Ownership for the legal person issuing the shares, rather than the real ultimate beneficial owner.

However, it should be noted that this service may present a lower risk when it is used for administrative purposes during the company formation period and the shares are transferred when sold.

3.1.6 Multiple services provided by the TCSP to a single client

In Ireland, a TCSP may provide multiple services to a client. The risks of each of the individual services described above may be compounded if a TCSP provides multiple services to a client over a long period without any apparent commercial basis for the use of these services. If there is no apparent commercial basis for the services being provided and if they are being used to prevent identification of the ultimate beneficial owner, this could be indicative of money laundering. Multiple TCSP services may be used to place layers between the company and the beneficial owners and, additionally, providing services to offshore beneficial owners and/or intermediaries may present increased risk.

TCSPs may provide a full “brass plate” service to set up a company, including company officers, nominee shareholder, registered addresses and other administrative functions. Such a service may potentially be used by the clients of a TCSP in an attempt to conceal the underlying beneficial owner. There is also a concern that such companies could effectively be ‘shell’ companies.

However, the provision of multiple services does not automatically indicate a higher risk for ML. The provision of multiple services to the same client may increase the TCSP’s understanding of the client and its business practice and transactions. Some services, such as the TCSP acting as a company director, directly involve the TCSP in the client’s decision making, increasing the information to which the TCSP has access. As such, providing multiple services to a single client is not always indicative of higher risk and may be a mitigating factor in terms of risk management.

3.1.7. Inherent Risk of ML risk rating

Different TCSP services provide varying inherent risk of money laundering as the various services obscure the beneficial ownership or origins of funds to different degrees. Combining different services may increase or decrease the risk of money laundering. All of these considerations are factors in determining a sector-wide risk rating for TCSPs.

As a whole, TCSP services are considered to present a **Significant (3) Inherent Risk for ML** based on the EU’s SNRA rating scale.

3.2 Inherent Risk of Terrorist Financing

The European Commission, in the EU Supranational AML/CFT risk assessment[24] noted that criminals may seek to set up opaque structures that can circumvent any restrictive measures in place. The assessment of the terrorist financing threat related to the creation of legal entities and legal arrangements shows that terrorist organisations may have difficulty in creating such structures. This is because these terrorist organisations are usually on the sanctions list. The more the terrorist organisation wants to hide its beneficial ownership identity, the more sophisticated the process needs to be. Knowledge of both domestic and international regulatory and taxation rules is required to create these structures which entail a high level of knowledge that can only be provided by professional intermediaries. It notes that law enforcement agencies and financial intelligence units have identified some simple methods that involve perpetrators using bank accounts and professional intermediaries to help them set up structures quickly and easily in order to gather cash to finance terrorist activities.

Therefore, the ability to create legal entities and legal arrangements is relevant for the terrorist financing threat, although only a limited number of such cases have been reported by law enforcement.The Commission concluded that few cases of using these methods to finance terrorism had been identified. This may be because the high level of technical expertise and knowledge required dissuades terrorist organisations that would prefer simpler and more accessible solutions, albeit the technical expertise provided by a TCSP may nullify this somewhat. The Commission considers the level of terrorist financing threat related to the creation of legal structures as moderately significant (level 2).

While TCSPs could, like any other corporate entity, be misused for TF purposes, we have not found anything specific to their activities that would increase the risk of their misuse for TF. Nor is there anything specific regarding the geography of TCSP's customers or their distribution channels that would indicate a higher risk for TF. On the other hand, clients of TCSPs may be located extra-jurisdictionally and, as noted above, may use TCSP services to obscure beneficial ownership. This may make the investigations more complex for law enforcement. Furthermore, if the beneficial ownership of legal persons is obscured, there is a possibility that the true beneficial owners may be located in jurisdictions where terrorist groups are prevalent, or that are high risk for terrorist activity.

TCSP services are considered to present a **Moderately Significant (2) Inherent Risk for TF** based on the EU's SNRA scale.

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN

4. Remaining Vulnerabilities of TCSPs

This document now considers the mitigants that serve to prevent TCSPs from having their business used for money laundering and/or terrorist financing purposes. Some of these mitigants are common to all TCSPs and these are set out initially. There are also some common residual risks. Then, taking those common mitigants as being in place, we look at the specificities relating to the various competent authorities that supervise TCSPs. As the supervisory practices conducted by the various competent authorities are mitigants in themselves, we have assigned individual Vulnerability ratings to each of the separate cohorts.

4.1 Common Mitigants for Money Laundering across all TCSPs

A TCSP is defined as a designated person under Section 25(1) of the CJA 2010 as amended. The CJA 2010 as amended contains many provisions that must be complied with by designated persons, including TCSPs. These obligations provide a defence mechanism against a business being used for money laundering and terrorist financing.

Table 8: Overview of the TCSP's legal obligations under the CJA 2010 as amended

Section of CJA 2010 as amended	Obligation on the Designated Person	Offence
Section 30A	Documented Risk Assessment document - identify and assess the risks of money laundering and terrorist financing in relation to the business	A designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment to a fine or imprisonment not exceeding 5 years (or both).
Section 30B	Assessment of risk in relation to a customer or transaction in determining the measures to be applied in relation to customer due diligence	A designated person who fails to document a determination in accordance with a direction under subsection (2) commits an offence and is liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment to a fine or imprisonment not exceeding 5 years (or both).

Section of CJA 2010 as amended	Obligation on the Designated Person	Offence
Section 33	Customer due diligence (CDD) - Identification and verification of customers and beneficial owners. Timing of CDD (prior to commencing relationship or carrying out transaction/service). Electronic Money Derogation provisions (where applicable.)	A designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 35	Special measures applying to business relationships.	Except as provided by section 36, a designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 36A	Examination of background and purpose of certain transactions	A designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 37	Enhanced CDD — politically exposed persons.	A person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 38A	Enhanced CDD for high risk third countries	A designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

Section of CJA 2010 as amended	Obligation on the Designated Person	Offence
		(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 39	Enhanced CDD in cases of heightened risk	A designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 40	Reliance on other persons to carry out CDD	A designated person who relies on a relevant third party to apply a measure under section 33 or 35(1) remains liable, under section 33 or 35(1), for any failure to apply the measure.
Section 42 & Section 49	Requirement for designated persons and related persons to report suspicious transactions and not to tip off or make a disclosure that could prejudice an investigation	s.42: Except as provided by section 46, a person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both). s.49: A person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 54	Internal policies and procedures and training	A designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Section of CJA 2010 as amended	Obligation on the Designated Person	Offence
Section 55	Keeping of records by designated persons.	A designated person who fails to comply with this section commits an offence and is liable— (a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

As set out above, obligations under the CJA 2010 as amended requires TCSPs to adopt internal policies, controls and procedures in relation to their business to prevent and detect ML/TF. They are also required to risk assess their own business as well as their clients and transactions. TCSPs are also obliged to maintain records evidencing the procedures applied and information obtained when effecting policies. The CJA 2010 as amended requires these policies to address a number of factors at a minimum and to be kept under review by senior management. These measures serve to ensure TCSPs are aware of the risks and have appropriate policies and procedures in place.

Under the CJA 2010 as amended, when new customers are onboarded, the TCSP is required to conduct Customer Due Diligence (CDD). This involves identifying and verifying the customer based on independent source documents, identifying the beneficial owners and obtaining information on the purpose and intended nature of the business relationship. Furthermore, a TCSP must be clear on the identity of the beneficial owner of the company it is forming and it should be clear on the intended purpose of the company.

4.1.1 Authorisation of TCSPs, including fit and proper assessment

TCSPs supervised by the Central Bank and the AMLCU are subject to a rigorous authorisation process with the entirety of Chapter 9 of the CJA 2010 as amended, which contains 22 sections, dedicated to this topic. Under Chapter 9, the Minister for Justice can authorise a TCSP, but the term “Minister,” in this instance, also includes the Central Bank, which can exercise the functions of the Minister in relation to TCSPs that are the subsidiaries of regulated credit and financial institutions. It is an offence for a TCSP to operate without authorisation from the Minister or the Central Bank, unless supervised by a designated accounting body. An authorisation lasts for 3 years and is renewable after that time.

The authorisation provides for an application for authorisation to be made to the Minister (AMLCU) or the Central Bank and for a fit and proper assessment to be carried out by the AMLCU or the Central Bank on the principals or partners and beneficial owners of a TCSP. Authorisation involves consideration of whether those with key functions in the TCSP are “fit and proper” persons and whether the TCSP can be expected to comply with the obligations on TCSPs under the CJA 2010 as amended. Fit and Proper testing includes consideration of any past convictions for:

(i) money laundering;

(ii) terrorist financing;

(iii) an offence involving fraud, dishonesty or breach of trust as well as consideration of other relevant factors that are relevant to determining whether the person is otherwise.

The AMLCU and the Central Bank may refuse an application on specified grounds. These include:

- the provision of false information,
- concerns regarding fitness and probity of the owners or principal officers within the applicant firm,
- concerns that the applicant is so structured or organised that it is not capable of being supervised as a designated person under the CJA 2010 as amended.

Application forms issued by the AMLCU and the Central Bank for TCSPs include questions on the ownership structure of the TCSP, the TCSP services the applicant intends to provide, and how AML/CFT compliance is integrated, where relevant, within the wider group. The AMLCU and the Central Bank will revert to the applicant on any issues that become known during the application process.

As part of its review of the application, the Central Bank will utilise its knowledge of the parent (regulated credit or financial institution) of the applicant TCSP to ensure that any issues with the parent are taken into account when considering authorisation of the TCSP.

Section 90 of the CJA 2010 as amended provides that the AMLCU and the Central Bank may impose conditions when granting an application for authorisation which are considered necessary for the proper and orderly regulation of the TCSP services provided and in particular, from preventing the business being used to carry out ML or TF activities. A TCSP must comply with any conditions imposed or may appeal the imposition of conditions if it considers them unjust.

The AMLCU and the Central Bank may amend an authorisation at any time, including adding conditions and serving notice of the intention of doing so. It is an offence for the TCSP not to comply with any conditions imposed.

Chapter 9 of the CJA 2010 as amended (Section 97) also contains provisions for the revocation of authorisation granted to TCSPs and for appeals against decisions of the AMLCU and the Central Bank. It provides for an appeal Tribunal to hear appeals under this chapter. Statutory Instruments 474 and 475 of 2018 underpin the appointment of two individuals who provide the Appeal Panel services.[25] Chapter 9 also provides that the AMLCU and Central Bank shall establish and maintain a register of persons authorised to carry on business as a TCSP.

The AMLCU publishes a list of those TCSPs authorised or revoked in the preceding 12 months at least once a year in the official journal of the Government of Ireland (the Iris Oifigiúil). It also has a register of TCSPs available on its website.[26] The Central Bank publishes its register in the Iris Oifigiúil and maintains a register of its authorised TCSPs on its website.[27] Chapter 9 provides that it is an offence for a person to carry out business as a TCSP without holding an authorisation issued by the Minister or the Central Bank under this chapter.

[25] Available at: https://www.irishstatutebook.ie/eli/2018/si/474/made/en/print and https://www.irishstatutebook.ie/eli/2018/si/475/made/en/print respectively

[26] Available at: www.amlcompliance.ie

[27] Available at: http://registers.centralbank.ie/DownloadsPage.aspx

4.1.2. Authorisation of Accountants acting as TCSPs

Section 84 of the CJA expressly excludes accountants from the definition of TCSP for the purpose of Chapter 9: *"trust or company service provider" does not include any of the following:*

(a) a member of a designated accountancy body;

(b) a barrister or solicitor;

(c) a credit institution or financial institution."

The Third Money Laundering Directive 2005/60/EC (3AMLD) set out in Article 1[28] that the designated persons covered by the Directive included accountants and legal professionals and then it also referred to trust or company service providers not already covered by those two categories. The explanatory memorandum to the Bill establishing the CJA 2010 as amended reflects this and in relation to section 84 notes that *"Section 84 defines a number of terms used. In particular, it defines the term 'trust or company service provider' to exclude a member of a designated accountancy body, a barrister or solicitor, or a credit institution or financial institution, as these categories are already subject to regulation."*[29]

Accountants acting as TCSPs are already regulated for their accountancy services and are distinct from standalone TCSPs, which need to be separately authorised and regulated by the Minister for Justice or the Central Bank. Nevertheless, they are subject to supervision for the TCSP activities they undertake separate to their primary role as an accountant. Under the MoU with the AMLCU, solicitors who establish a TCSP as a company are subject to authorisation and supervision by the AMLCU, while in three of the scenarios set out in Table 1 on Page 6, accountants are subject to supervision by the DABs.

The DABs under Section 63A of the CJA 2010 as amended are required to take the necessary measures to prevent anyone convicted of a "relevant offence" from performing a management function in or being a beneficial owner of an external accountancy practice. A relevant offence means an offence under the CJA 2010 as amended, an offence specified in Schedule 1 of the Criminal Justice Act 2011 or an offence under the law of a place, other than the State, which if done in the State would constitute an offence under the CJA 2010 as amended or the Criminal Justice Act 2011.[30] Offences under Schedule 1 of the Criminal Justice Act 2011 are extensive and include offences relating to banking, investment of funds and other financial activities, company law offences, money laundering and terrorist financing offences, theft and fraud offences, consumer protection offences, and criminal damage to property offences.

Any person performing a management function or being the beneficial owner of an accountancy practice must inform the relevant competent authority within 30 days. Chartered Accountants Ireland provides for a registration process for TCSPs for these purposes.[31] There is no legal requirement for the DABs to make available publicly a list of TCSPs they supervise, and no such public list has been published to date.

---

[28] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02005L0060-20110104

[29] Available at: https://data.oireachtas.ie/ie/oireachtas/bill/2009/55/eng/memo/b5509d-memo.pdf

[30] Available at: https://www.lawreform.ie/_fileupload/RevisedActs/WithAnnotations/HTML/en_act_2011_0022.HTM

[31] Available at: https://www.charteredaccountants.ie/docs/default-source/dept-professional-standards-(psd)/support-and-guidance/AML/guidance-to-the-money-laundering-supervision-regulations-2020.pdf?sfvrsn=6

4.1.3. Beneficial ownership

When a corporate or legal entity is incorporated in the state, information on the company's beneficial owners must be filed with the Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies (RBO).[32] The European Union (Anti-Money Laundering: Beneficial Ownership Of Corporate Entities) Regulations 2019 (SI 110 of 2019) sets out the legal obligations to do so.[33] ICAVs and certain financial vehicles ae the only corporate entities not required to submit beneficial ownership information to the RBO, as their information is submitted to a separate register (please see below). An Garda Síochána, FIU Ireland and all the competent authorities under the CJA 2010 as amended are authorised to access the full information held in the RBO. Others, including members of the public, may pay a small fee to access a limited amount of information held in the Registers. Information from the Registers must be checked for Customer Due Diligence purposes by a designated person, but they cannot rely exclusively on the information from the Register for this purpose and must do other checks. Significant penalties may be imposed for breaches of the regulations. These obligations to register beneficial ownership information in a central register help mitigate the possibility of corporate entities being misused for ML/TF at a high level.[34]

A TCSP set up as a company must therefore file its beneficial ownership information on the RBO. Where the TCSP has clients that are companies, the companies' data must also be filed centrally on the RBO and the TCSP, as part of its due diligence under Section 33 of the CJA 2010 as amended, is required to examine the RBO. Upon registration, the Registrar for the RBO, the Companies Registration Office, carries out a cross-check on the beneficial owner's PPS Number (where he/she is an Irish citizen) but does not otherwise verify the accuracy of the information provided. A TCSP must not only check the register and see if it matches the information provided by the client, but also probe the accuracy of the information with the client to ensure it has correctly identified the beneficial owner. The obligation to check the identity of the beneficial owner provides a mitigant against the misuse of the TCSP's services.

Similar beneficial ownership provisions apply in relation to trusts. The European Union (Anti-Money Laundering: Beneficial Ownership of Trusts) Regulations 2021 (S.I. 194 of 2021)[35] require that information on a trust (trustee, settlor, beneficiary etc.) must be filed centrally to a register maintained by the Revenue Commissioners. Competent Authorities, as well as An Garda Síochána (AGS) and FIU Ireland, have full access to this register. Significant penalties may be imposed for breaches of the regulations. These obligations to register beneficial ownership information in a central register help mitigate the possibility of trusts being misused for ML/TF.

In addition, the European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of Certain Financial Vehicles) Regulations 2020 (S.I.

[32] Further details on the RBO are available at: https://rbo.gov.ie/about.html#:~:text=The%20Register%20of%20Beneficial%20Ownership%20(RBO)%20is%20the%20central%20repository,are%20their%20beneficial%20owners%2Fcontrollers

[33] Available at: https://www.irishstatutebook.ie/eli/2019/si/110/made/en/pdf

[34] See Legal Persons and Legal Arrangements Risk Assessment for a more detailed discussion on this: https://assets.gov.ie/75052/d586a59d-2f1d-48b6-b1cc-857c9316cc42.pdf

[35] Available at: https://www.irishstatutebook.ie/eli/2021/si/194/made/en/pdf

No. 233/2020)[36] provided for the modification of S.I. 110 of 2019 to create registers of various financial vehicles, including Irish Collective Asset Management Vehicles. Some of these entities may be clients of TCSPs. This financial vehicle register is managed by the Central Bank. Again, the data on beneficial ownership of these vehicles registered with the Central Bank is available to AGS, FIU and competent authorities. These obligations to register beneficial ownership information in a central register help mitigate the possibility of certain financial vehicles being misused for ML/TF.

4.1.4 Domestic Co-operation

The terms of reference for the Anti-Money Laundering Steering Committee (AMLSC) were reviewed in 2021. As part of this review, the membership of the AMLSC was expanded to include the DABs and other relevant private sector representatives. Additional Government Departments have also joined the AMLSC, allowing a broader range of stakeholders to address AML/CFT concerns. Expansion of the membership allows the AMLSC to share information and facilitate communication, discussion and feedback between domestic stakeholders regarding emerging trends and risks, developments in international standards, and in AML/CFT legislation at EU, national and international levels.

All competent authorities responsible for supervising TCSPs are now represented on the AMLSC, which allows emerging risks and trends to be rapidly shared across the framework. The AMLSC also permits a feedback loop for competent authorities and the FIU, whereby issues with STRs can be raised and passed on to the TCSPs by their supervisors.

4.2 Mitigants for Money Laundering and Terrorist Financing by each TCSP Supervisor

Another means by which risk is mitigated generally is through supervision of TCSPs by the relevant competent authorities. All competent authorities have an obligation under section 63 of the CJA 2010 as amended to effectively monitor the designated persons that they supervise and to take measures to secure their compliance with the CJA 2010 as amended. Under Section 63C of the CJA 2010 as amended, all competent authorities must adopt a risk-based approach to supervision and base the frequency and intensity of onsite and offsite supervision on the risk profile of the TCSPs.

As a result of the assessment of different TCSPs, the supervisory regimes they are subject to, and the nature of the owners and customers, separate TCSP risk ratings have been assigned to those TCSPs that are subsidiaries of the regulated financial sector and those TCSPs that are not.

Effective supervision includes ensuring TCSPs are not just ticking boxes in relation to AML/CFT compliance, but have considered any unique or individual factors in relation to the services they are providing to their customers. Considerations should include:

- The frequency of business requests,
- The commercial purpose of the client, and whether requests are related to this purpose

[36] Available at: https://www.irishstatutebook.ie/eli/2020/si/233/made/en/print

- The location of any intermediaries or subsidiaries of the customer and whether this presents higher risk,
- Any individual requests that appear questionable, such as the formation of a large number of companies at once,
- Regular referral to risk indicators and typologies and reviewing the structure and activity of their clients on this basis.

This list is not exhaustive and considerations will vary depending on the specifics of both the TCSP and its clients.

Table 9: Number of Inspections by each Supervisor 2018-2020.

	Number of TCSPs[37]	2018 Onsite	2018 Offsite	2019 Onsite	2019 Offsite	2020 Onsite	2020 Offsite	Total 2018-2020	Total % 2018-2020
CBI	33	4	0	2	0	0	0	6	18%
AMLCU[38]	356	75	0	85	0	62	0	160	45%
DABs	388	66	0	84	0	12	34	196	51%

4.2.1. Central Bank of Ireland

Oversight and Supervision

The Central Bank applies a risk-based approach to supervision, which involves two elements:

- Identification and assessment of ML/TF risk exposure of the sector/firm; and
- Specific supervisory engagement on AML/CFT elements to monitor compliance with AML/CFT obligations and where weaknesses are identified requiring remediation to ensure compliance.

Consistent with the rating applied to the TCSPs it supervises and in line with its risk based approach to supervision, the Central Bank adopts a spot check and responsive strategy in carrying out engagements with TCSPs in its population, as well as requiring firms to complete a risk evaluation questionnaire annually. Consequently, four inspections took place in 2018, two took place in 2019, none took place in 2020 and two review meetings took place in 2021.

The inspections and review meetings held with TCSPs were full-scope engagements, which examined the robustness of the AML/CTF Control Framework of the TCSP. This included assessment of the quality of AML/CFT policies and procedures, governance framework, risk assessment, training, customer due diligence, transaction monitoring and record keeping. Where weaknesses were identified during engagements, the Central Bank issued remediation programmes, which are followed up on until the weaknesses are fully remediated.

Following the six inspections, two TCSPs were rated 'ineffective'— the lowest rating on the CBI's rating scale— and three were rated 'weak' due to the vulnerabilities in relation to beneficial ownership transparency, risk assessment, CDD and AML/CFT policies and

[37] As of July 2021.

[38] In November 2020, the AMLCU also commenced a thematic offsite inspection of all the TCSPs it supervises.

procedures. However, the Central Bank did not consider findings requiring remediation to be significant in nature and reported that all were addressed by firms in a timely manner.

In addition, all 33 of the TCSPs were issued with a Risk Evaluation Questionnaire ('REQ') for completion in 2021. The REQ is a detailed questionnaire that provides the Central Bank with an insight into the following aspects of TCSPs:

- **Governance** – Board/Senior management oversight, risk assessment, policies and procedures and training and record keeping
- **Risk Profile** – products and services, geography, distribution channels, customer exposure and Politically Exposed Persons and financial sanctions
- **Risk Based Approach** – policies and procedures, assurance testing, third party reliance and outsourcing
- **Suspicious activity** – investigate/escalate suspicious activity
- **Management information** – report management information

The 2021 REQs were reviewed by the Central Bank as part of its supervisory engagement model.

In September 2017, the Central Bank hosted a seminar to which all those TCSPs supervised by the Central Bank were invited. At the seminar, the Central Bank shared the findings from the programme of supervisory engagements undertaken up to that point, as well as outlining its compliance expectations. In 2019, a Dear CEO letter issued to the TCSPs in its cohort which outlined a number of weaknesses identified by the Central Bank in its cohort's AML/CFT control frameworks.[39] The letter advised CEOs of TCSPs that the Central Bank expected the content of the letter to be carefully considered and brought to the attention of the board/senior management to ensure any issues contained therein are addressed. TCSPs were also reminded of the key obligations to establish and maintain frameworks tailored to mitigate AML/CFT risks inherent in their specific business activities and to position themselves to demonstrate to the Central Bank that all reasonable steps have been taken to ensure compliance with the requirements of the CJA 2010 as amended.

Risk Assessment

The Central Bank examines the business risk assessments of TCSPs it supervises when conducting inspections. A number of TCSPs relied on group-wide risk assessments co-ordinated by the parent entity which, on occasion, failed to reference the risks specific to their TCSP activities. These TCSPs were followed up with post-inspection engagements and now have appropriate risk assessments in place.

Customer Due Diligence

The TCSPs in the Central Bank's cohort rely on their parent company's staff for their day-to day operations, meaning that the customer due diligence framework applied on an initial and on an on-going basis was that of the parent. As the parent of the TCSP was also likely to have a business relationship with customers of the TCSP, or the customer would be the parent entity itself, CDD documentation and information was collected and updated by the staff of the

[39] Available at: https://www.centralbank.ie/docs/default-source/regulation/amld-/dear-ceo-letter---compliance-by-trust-or-company-service-providers-with-their-obligations-under-the-criminal-justics-act-2010.pdf?sfvrsn=6

parent in response to changes and events during the life of each business relationship. As the parent's typical business relationship with each customer is investment advice and retirement planning, customers are typically Irish resident and of long standing with the parent. Reliance on third parties, within the meaning of Section 40 of the CJA 2010 as amended, is not a feature of their business.

Policies, Controls, and Procedures

A large number of TCSPs in the Central Bank's cohort were found to be dependent on their parent entity's AML/CFT polices, controls and procedures. While this is potentially a vulnerability, the parent entities are designated persons in their own right and their policies and procedures were of sufficiently high standard. This mitigated the vulnerability in these instances to a large degree. In addition, customers of these TCSPs tend to either be the parent entity itself or customers of the parent entity. This weakness was also highlighted as part of the Dear CEO letter issued to the sector in 2019 and therefore should not be prevalent in the sector.

As transactions and customer facing activities are carried out by the staff of the parent, the training on suspicious transactions, transaction monitoring and reporting process reflected the practices and systems of the parent. These systems and processes therefore reflected the general quality of STR frameworks in the parent's sector. All firms provided staff with information on their STR process through their policies and procedures and through training. This documented how staff should (i) raise an STR; and (ii) submit the STR to AGS and the Revenue Commissioners.

As the TCSPs relied on the staff of their parent for their day-to day operations, regular training was governed by the training policies of the parent. The level of training therefore reflected the general quality of training in the parent. This training was generally of a high standard in light of the higher ML risk of the parent's sector. Staff are required to complete a test or answer a series of questions to demonstrate their understanding of AML requirements. Specific and bespoke training was provided to staff that had an increased exposure to ML risks.

Remaining Vulnerability rating

Given the unique characteristics of the Central Bank's cohort of TCSPs, they are considered to present a lower vulnerability of ML/TF.

Taking account of the mitigants set out above, overall the level of:

- **ML Remaining Vulnerability** for TCSPs supervised by the Central Bank is assessed to be **Lowly Significant (1).**
- **TF Remaining Vulnerability** for TCSPs supervised by the Central Bank is assessed to be **Lowly Significant (1).**

4.2.2. The Designated Accountancy Bodies

Five DABs supervise TCSPs in accordance with the Memorandum of Understanding set out in Table 1. The responses provided by the DABs to the questionnaire indicated a mixed understanding of TCSP obligations and risks amongst DABs. A number of DABs indicated that the TCSPs they supervise are typically already registered with the DAB as accountants

and asserted that this lowers the ML/TF vulnerability of such TCSPs. However, it is notable that the United Kingdom's National AML/CFT Risk Assessment (last updated in 2020) assessed Trust or Company Service Providers as posing a high risk, with that risk increasing when TCSP services are provided with other financial, legal or accountancy services.[40] It is also notable that the UK considered TCSPs as a low risk for terrorist financing.

Inspection Process

The questionnaire responses returned by the DABs indicate that four out of five of the Designated Accountancy Bodies have inspected TCSPs at least once in the last three years. The fifth conducted a thematic review of their cohort in 2020 focusing on beneficial ownership and corroborating information provided to the RBO by the TCSPs. Moreover, two DABs report only inspecting TCSPs for the first time in 2020. The questionnaire responses as a whole indicated that the DABs apply the risk-based approach, with higher risk TCSPs being inspected more frequently. A number of DABs conduct overall compliance inspections, which covers accounting and TCSP services, while others conduct specific TCSP AML inspections.

While the former approach is acceptable, the DABs must ensure that these inspections adequately assess AML/CFT frameworks in respect of TCSP services. One DAB in particular demonstrated a clear procedure and approach to inspections which included a pre-visit questionnaire, a detailed discussion of the TCSP's policies, procedures and risks and a closing meeting to formally communicate detailed findings (with a response required within 14 days). On the other hand, another did not detail its inspection process at all and had only inspected a TCSP for the first time in 2020. As such, it is evident that the approach to inspections and supervision by the DABs as a whole is not necessarily sufficient to assess the risks on a consistent basis.

Oversight and Supervision

The questionnaire responses returned by the DABs indicated that some DABs had good knowledge of the risks associated with TCSP activities and they explained how they tailor inspections or general supervision to take TCSP risks into account. However, other DABs did not demonstrate an appreciation of TCSP risk factors. While it is possible that these risk factors simply are not common among their cohort, there is limited evidence that this has been examined. A lack of clarity on the supervisors' part does not indicate higher vulnerability *per se*, but it does indicate that some inherent risk factors may not be examined to the degree that the inherent risk of TCSP activities necessitates. This applies even to the supervisors that have conducted a higher number of inspections.

A possible residual risk is that some accountants may be providing TCSP services, without understanding that the services mean they are acting as TCSPs and should register for these with the DAB separately to accountancy services and be supervised for AML/CFT purposes as a separate category of business activity. The DABs indicated that their membership is asked whether they provide TCSP services on annual returns and similar communications. This is then verified by checking their Members' websites to see what services they advertise, or by asking them to specifically answer a question on whether they provide the services listed in the definition of a TCSP. Transparency of the TCSPs supervised by DABs and of whether

[40] Available at: https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

all those accountants providing TCSP services are properly registered and supervised by a DAB, would be improved by having a public list of TCSPs supervised by the DABs, as exists for the AMLCU and Central Bank.

The DABs have confirmed that all have full access to the RBO. Two confirmed in questionnaire responses that they use it to assist with compliance checks, and most of the DABs indicate the use of online search systems such as FAME, which allow access to the same information. However, they did not indicate the extent to which they probe the data that TCSPs have provided to the RBO as part of their supervision process.

All DABs examine TCSP business risk assessments when conducting inspections. However, the number of inspections conducted by each individual supervisor varies considerably as advised above. All DABs indicate that they review CDD during a visit or desk-based review process and report that the TCSPs they supervise carry out CDD in general. It is very uncommon for TCSPs supervised by the DABs to outsource customer due diligence requirements, with only two reporting that they were aware of it happening at all (in both cases, the percentage of their cohort doing so was under 5%).

All of the DABs listed TCSPs implementing policies and procedures as required under the CJA 2010 as amended. However, DABs reported that whilst the majority of firms/practices do meet the required standards, a small number had not. Inadequate AML policies and procedures are one of the main deficiencies highlighted during inspections. The reasons are varied, including inadequate staff training on AML/CFT procedures, improper documentation, failure to carry out or implement documented policies in practice, ongoing CDD improperly documented, and internal ML compliance reviews either not completed or ineffective. The DABs explained that following an inspection, the firm/practice may be required to undertake remedial action, which is then reviewed by the DAB.

Remaining Vulnerability rating

Generally, the extent of supervision and the understanding demonstrated of specific TCSP risks varies significantly across the DABs.

Taking account of the mitigants set out above, overall the level of:

- **ML Remaining Vulnerability** for TCSPs supervised by the DABs is assessed to be **Significant (3).**
- **TF Remaining Vulnerability** for TCSPs supervised by the DABs is assessed to be **Moderately Significant (2).**

4.2.3. Anti-Money Laundering Compliance Unit (AMLCU, Department of Justice)

Oversight and Supervision

The AMLCU is the supervisor by default for TCSPs that do not fall to be supervised by either the Central Bank or the DABs. A register of TCSPs authorised at any given time by the AMLCU is publically available on its website.[41] The cohort supervised by the AMLCU also reflects the two Memoranda of Understanding with the Law Society and with the DABs.

[41] Available at: https://www.amlcompliance.ie/registers/

As the AMLCU, rather than the Law Society, supervises TCSPs when a solicitor sets up a TCSP as a limited company, the AMLCU supervises a significant number of TCSPs that have been established by solicitors. As noted in the memoranda, the Law Society is responsible for supervising the solicitor when it provides trust and company legal services to a TCSP.

FATF has noted that the functions of TCSPs can vary greatly. TCSPs may provide a significant, varied range of services and activities, influenced by the clients they serve, as well as the size, focus, ownership profile and sophistication of the firm. Consistent with this the AMLCU reports that it supervises a highly varied cohort of TCSPs, which face different risks depending on several factors.

In this regard, the TCSPs supervised by the AMLCU provide services such as:

- Providing Pension Trustee services where the pension fund is regulated by the Pensions Authority;
- Providing incorporation services i.e. setting up companies and other bodies corporate, or providing business office services (address etc.);
- Providing trustee services, sometimes low-risk and other times higher risk;
- Providing directorship services or company secretary services; and
- Providing nominee services (including nominee shareholder services).

The scale of these TCSPs can vary significantly also with some having a small number of clients while others may have hundreds of clients.

The client services for these TCSPs' clients may be straightforward or complex. Some clients may be publicly listed firms (considered lower risk), or may be providing straightforward local services to local clients with whom they have an established business relationship (e.g. pension trustee services or office services).

Clients of TCSPs may have low or high turnover, with considerable variation. Some clients of TCSPs supervised by the AMLCU are unregulated Special Purpose Vehicles (SPV), including Collateralised Loan Obligations (CLOs), or are orphan structures. The latter are trust structures that separate the beneficial ownership in remainder— usually a charity— to the beneficiaries of the economic activity of the trust. Some TCSPs may have clients with structures that cross a number of jurisdictions. Some TCSPs have clients that are discretionary trust structures where the beneficiary can be changed at the discretion of the trustee. Some TCSPs may have lower risk characteristics in terms of the services provided e.g. bespoke set up of a company for an Irish owner manager firm. Others, with hundreds of clients, may have complex structures and layers, with elements in other jurisdictions including outside the EU, and where some of the clients appear to have at least one common structural layer.

The AMLCU has some TCSPs that operate nominee arrangements for the clients. The TCSP may provide nominee Directors - these are understood to be appointed mainly due to an entity being from outside the EEA and the legal entity may have no tangible connections with Ireland. In company law, a nominee Director has the same obligations as a Director. In that regard, legally the TCSP providing nominee Director services needs to have good knowledge of the company, its purpose and activity. As a supervisor, the AMLCU will check if this is the case and if the TCSP is able to demonstrate satisfactory understanding. A TCSP may also provide nominee shareholdings, which may obscure beneficial ownership. There is currently no legal obligation on a nominee to disclose this status unless asked a direct question by the supervisory body.

The AMLCU notes that some of the TCSPs supervised may have no employees (e.g. a legal firm may second staff to work part-time to fulfil TCSP duties or the TCSP may be providing a service to another related TCSP) or a very small number of employees (e.g. 1 or 2) and typically TCSP turnover would be low., , An analysis by the AMLCU of 157 TCSPs highlighted that 120 of them had declared an annual turnover of less than €15,000 per annum.

On the other hand, TCSPs may hold client assets or provide services to clients that have billions of euro passing through them. For example, One TCSP inspected in early 2020 had a client structured as a special purpose vehicle established under section 110 of the Taxes Act that was found to have €32 billion in funds going through it. The CLO market in Ireland expanded significantly in April 2021 following tax changes in the Netherlands. The majority of these SPVs are not regulated in Ireland. One media report from 2021 calculated the value of approximately 414 vehicles as €153 billion.[42] These CLOs tend to avail of the services of TCSPs, which fall to the AMLCU for supervision. The scale of funds that the clients of TCSPs are dealing in does not necessarily provide any indication of anything untoward, or of ML or TF; however it does indicate that some TCSPs supervised by the AMLCU are dealing with complex high value clients involved in international markets.

Inspection Process

The AMLCU adopts a risk-based approach to supervision of TCSPs. Complex TCSPs and those that have higher risk factors associated with them are considered higher risk and are subject to more in-depth inspection and questioning. As set out above, the AMLCU engages in an extremely detailed authorisation process, which includes fit and proper checks (including police vetting) and reviews of due diligence databases and open data searches. Authorisations by the AMLCU must be renewed every three years.

In order to assess the risks of the TCSP under the CJA 2010 as amended, the AMLCU conducts onsite compliance inspections. At each inspection, the AMLCU inspecting officer expects to see evidence of risk assessments having been conducted and that the risk assessment has been approved at senior management level. Records of current and historical risk assessments (maintained for a minimum of five years) must be available to the inspecting officer on request. An in-depth discussion of the risk factors will also take place between the inspecting officer and the TCSP staff during the inspection to assess the level of knowledge and understanding of risk factors. If the risks have not been identified adequately by the TCSP and/or appropriate mitigating measures applied, the TCSP will be found non-compliant and will have to demonstrate that it has modified its business risk assessment to appropriately take account of risk. Clients and transactions must also be risk-rated under section 30B of the CJA 2010 as amended and the AMLCU has issued a direction[43] to TCSPs outlining that the risk assessment of clients and transactions must be documented.

During a compliance inspection by the AMLCU, a TCSP must demonstrate that it understands its clients and the purpose of the services it is providing to its clients. It must be able to demonstrate that it examines the background and purpose of all complex and unusually large transactions and all unusual patterns of transactions. It will be asked to demonstrate that any transactions fitting this description have been examined and escalated to senior management

[42] https://www.irishtimes.com/business/financial-services/how-dublin-quietly-became-dumping-ground-for-some-of-europe-s-riskiest-corporate-loans-1.4527161

[43] AMLCU-Direction-Under-Section-30B.pdf (amlcompliance.ie)

for review and approval and, where applicable, that the risk rating of the customer was amended and a suspicious transaction report was submitted, where appropriate.

The AMLCU checks underlying beneficial ownership information and that the TCSP can illustrate its own beneficial ownership and the beneficial ownership information of its clients. Where senior managing officers in the TCSP are identified as the beneficial owner, the AMLCU will probe why this is so and why the underlying beneficial owner could not be identified. The AMLCU carries out a detailed background check on the TCSP being inspected prior to the day of inspection, such as checks on the CRO and RBO registers.

The AMLCU's approach for conducting inspections is detailed and comprehensive and this is an important mitigation factor in terms of the risks associated with some of the TCSPs supervised by the AMLCU. The AMLCU carried out onsite inspections on 75 TCSPs in 2018, 85 in 2019, 62 in 2020 and 134 in 2021. A TCSP inspected by the AMLCU is risk rated post inspection on the basis the findings in terms of compliance with the CJA 2010 as amended. However, even if a TCSP demonstrated full compliance, it may be considered inherently risky due to its complexity or the nature of its business and still be allocated a high risk rating.

The AMLCU also carried out a thematic inspection of all TCSPs in November 2020, whereby it sought the same set of data from all TCSPs, including the number of employees, turnover and information on clients and their beneficial ownership. All returns were individually reviewed and assessed in 2021, with the purpose of giving a clearer overall picture of the risks associated with the AMLCU TCSP cohort. Overall, the AMLCU's approach for conducting inspections is detailed and comprehensive.

FATF notes that TCSPs need to make reasonable judgements that reflect their particular services and activities as risk varies considerably depending on factors such as size, complexity of clients etc. Appropriate mitigation measures depend on the nature and risks arising from the TCSP's role and involvement in the affairs of its clients. Circumstances may vary considerably between TCSPs e.g. between those that represent clients directly as trustees or directors, controlling the affairs of the legal arrangement or legal person and those that are engaged for distinct purposes, such as the provision of registered office only services, and that have to rely on information on the client's activities from external directors. Due to the different nature of the TCSPs supervised by the AMLCU, some of the TCSPs are considered low risk, some medium and some high risk.

Remaining Vulnerability rating

Taking account of the mitigants set out above and in view of the range of TCSPs supervised, overall the level of:

- **ML Remaining Vulnerability** for TCSPs supervised by the Anti-Money Laundering Compliance Unit is assessed to be **Moderately Significant (2).**
- **TF Remaining Vulnerability** for TCSPs supervised by the Anti-Money Laundering Compliance Unit is assessed to be **Lowly Significant (1).**

5. Residual Risk

This section considers the residual risks, which are applicable to all TCSPs. As demonstrated in Section 4, there are common mitigation measures and then additional factors and mitigation actions applied by each competent authority. Due to this, we then calculate a residual risk rating for the TCSPs overseen by each supervisor in line with the EU SNRA Methodology.

5.1 Money Laundering Common Residual Risks

5.1.1. Full list of TCSPs operating in Ireland

One issue apparent from this risk assessment is that, unlike the Central Bank and the AMLCU, the DABs do not publish lists of the TCSPs they supervise. To help ensure that all those operating as TCSPs are supervised by the Central Bank, AMLCU or DABs, the DABs should publish the list of those TCSPs that they supervise. This would create greater transparency as to all of the TCSPs that are operating in Ireland.

5.1.2. Use of Senior Managing Official Provision – where beneficial owner cannot be identified

Article 3(6)(a)(ii) of 4AMLD (transposed into Irish law by Section 33 of the CJA 2010 as amended) provides that if, after having exhausted all possible means and provided there are no grounds for suspicion:

- no beneficial owner is identified,
- or if there is any doubt that the person(s) identified are the beneficial owner(s),

the Register for Beneficial Ownership of Corporate Entities may include the natural person (or persons) who hold the position of senior managing official (or officials). Designated Persons, including TCSPs, are required to keep records of the actions taken in order to identify the beneficial ownership. However, sometimes where a TCSP is providing director services trustee service, nominee shareholder or nominee director services, the senior managing officials of the TCSPs may be listed as the beneficial owner of the client's company or trust in lieu of the true underlying beneficial owner, with the TCSP arguing that the true beneficial owner could not be identified (e.g. orphan structure).

It is a vulnerability if this provision around senior managing officials could be used by TCSPs to obscure the real ultimate beneficial owner of a legal entity or arrangement. Supervisors, when sampling clients and the CDD carried out, need to not only check the register but also probe the beneficial ownership information related to the TCSP's clients to ascertain the accuracy of the data on the register. It is essential for supervisors to conduct rigorous follow-up with TCSPs to ascertain whether the TCSP can demonstrate adequate understanding of its clients, the beneficial owners of its clients and the purpose of the transactions they are facilitating. Enforcement action under the CJA 2010 as amended may also be necessary when this is not the case.

5.2 Terrorist Financing Common Residual Risks

While all of the TCSP services under the CJA 2010 as amended could be misused for the purposes of TF, the subcommittee has not identified any information to indicate that this happening in practice. While the AMLCU reported that a small proportion of its cohort has dealings with countries indicated as presenting geographical risk factors (based on Schedule 4 of the CJA 2010 as amended), no supervisor has reported a TCSP in its cohort that has a customer based in a jurisdiction considered high risk for terrorist activity, or where terrorist groups are prevalent.

5.3 Money Laundering and Terrorist Financing Residual Risk of TCSPs by Supervisor

5.3.1. Central Bank of Ireland

Based on the EU's SNRA rating scale, the Inherent ML Risk of the TCSP sector as a whole is deemed to be Significant (3), while the Remaining Vulnerability of the TCSPs supervised by the Central Bank, is rated Lowly Significant (1), placing the TCSPs supervised by the Central Bank at **1.8 for ML** on the scale.

The Inherent TF Risk of the TCSP sector as a whole is deemed to be Moderately Significant (2), while the Remaining Vulnerability for TF of the AMLCU's TCSPs is rated Lowly Significant (1), placing the TCSPs supervised by the AMLCU at **1.4 for TF** on the scale.

Inherent Risk (i.e. Threats and Vulnerabilities before mitigation)	**Very Significant**	2.2	2.8	3.4	4
	Significant	1.8 **ML Residual Risk**	2.4	3	3.6
	Moderately Significant	1.4 **TF Residual Risk**	2	2.6	3.2
	Lowly Significant	1	1.6	2.2	2.8
		Lowly Significant	**Moderately Significant**	**Significant**	**Very Significant**
	Remaining Vulnerabilities (i.e. taking account of the existence and effectiveness of safeguards)				

As a result, the Residual Risk of ML for the TCSPs supervised by the Central Bank is rated as **Medium-Low on the National Risk Assessment scale**.

As a result, the Residual Risk of TF for the TCSPs supervised by the Central Bank is rated as **Low on the on the National Risk Assessment scale**.

5.3.2. Designated Accountancy Bodies

Based on the EU's SNRA rating scale, the Inherent ML Risk of the TCSP sector as a whole is deemed to be Significant (3), while the Remaining Vulnerability of the TCSPs supervised by the DABS is rated Significant (3), placing the TCSPs supervised by the DABs at **3 for ML** on the scale.

The Inherent TF Risk of the TCSP sector as a whole is deemed to be Moderately Significant (2), while the Remaining Vulnerability for TF of the TCSPs supervised by the AMLCU is rated Moderately Significant (2), placing the TCSPs supervised by the AMLCU at **2 for TF** on the scale.

Inherent Risk (i.e. Threats and Vulnerabilities before mitigation)	**Very Significant**	2.2	2.8	3.4	4
	Significant	1.8	2.4	3 **ML Residual Risk**	3.6
	Moderately Significant	1.4	2 **TF Residual Risk**	2.6	3.2
	Lowly Significant	1	1.6	2.2	2.8
		Lowly Significant	**Moderately Significant**	**Significant**	**Very Significant**
	Remaining Vulnerabilities (i.e. taking account of the existence and effectiveness of safeguards))				

As a result, the Residual Risk of ML for the TCSPs supervised by the DABs is rated as **Medium-High on the National Risk Assessment scale**.

As a result, the Residual Risk of TF for the TCSPs supervised by the DABs is rated as **Medium-Low on the on the National Risk Assessment scale**.

5.3.3. Anti-Money Laundering Compliance Unit (AMLCU, Department of Justice)

Based on the EU's SNRA rating scale, the Inherent ML Risk of the TCSP sector as a whole is deemed to be Significant (3), while the Remaining Vulnerability for ML of the TCSPs supervised by the AMLCU is rated Moderately Significant (2), placing the TCSPs supervised by the AMLCU at **2.4 for ML** on the scale.

The Inherent TF Risk of the TCSP sector as a whole is deemed to be Moderately Significant (2), while the Remaining Vulnerability for TF of the AMLCU's TCSPs is rated Lowly Significant (1), placing the TCSPs supervised by the AMLCU at **1.4 for TF** on the scale.

Inherent Risk (i.e. Threats and Vulnerabilities before mitigation)	**Very Significant**	2.2	2.8	3.4	4
	Significant	1.8	2.4 **ML Residual Risk**	3	3.6
	Moderately Significant	1.4 **TF Residual Risk**	2	2.6	3.2
	Lowly Significant	1	1.6	2.2	2.8
		Lowly Significant	**Moderately Significant**	**Significant**	**Very Significant**
	Remaining Vulnerabilities (i.e. taking account of the existence and effectiveness of safeguards)				

As a result, the Residual Risk of ML for the TCSPs supervised by the AMLCU is rated **Medium Low on the National Risk Assessment scale**.

As a result, the residual risk of TF for the TCSPs supervised by the AMLCU is rated **Low on the National Risk Assessment scale**.

6. Recommendations

The functions and structure of TCSPs operating in Ireland vary considerably. This corresponds with FATF's finding[44] that TCSPs may provide a significant and varied range of services and activities, influenced by the clients they serve, as well as the size, focus, ownership profile and sophistication of the firm. As such, while this risk assessment has required high level assessments of risk, there is a wide spectrum of TCSPs operating in each category and some TCSPs may be considerably lower risk at an individual level than the ratings in the risk assessment might imply.

6.1 Authorisation Process and publication of TCSP Registers

One of the significant differences between the three types of TCSP supervisors is the in-depth authorisation process, specifically in relation to TCSPs and the transparency of those supervised. Both the Central Bank and the AMLCU operate a rigorous authorisation process and publish lists of those TCSPs supervised in Iris Oifigiúil (the State's official journal) and on their respective websites. While it is understood that the DABs undertake fitness checks on members generally, it is unclear whether any additional checks are carried out on those operating as TCSPs. Partly due to the lack of publication of TCSPs supervised by DABs, it is also unclear whether all accountants providing services that fit the definition of TCSP have been appropriately identified as TCSPs. Such a list would assist with identifying such TCSPs. Some DABs in the questionnaire returns expressed a view that the TCSP services being provided were low risk because the clients of the TCSP were clients to whom accountancy services were also being provided. However, it is unclear to what extent this is the case. In the NRA of at least one other jurisdiction, such TCSPs are assessed as being of higher risk and the European Commission has expressed particular concern about professionals providing trust and company services in Ireland's Country Specific Recommendation.

Recommendations:

(a) It is recommended that a full list of all TCSPs operating in the State be made publicly available. The DABs should publish the list of TCSPs supervised by each DAB and this should be raised with the DABs at the AMLSC. This would significantly improve transparency and accountability within this sector.

(b) It is recommended that DABs review their risk assessment of the provision of TCSP services where accountancy services are being provided to the same client to ensure that all ML/TF risks are appropriately identified and assessed. It is recommended that they also conduct a review of their current supervisory process with a view to addressing any additional risks that may be associated with those members operating as TCSPs, in view of the potential additional risks identified in this risk assessment and in view of findings in other jurisdictions and by the European Commission that the provision of both accounting and TCSP services may be riskier than just accounting services.

(c) It is recommended that consideration be given as to whether any additional guidance to identify members of the DABs potentially providing TCSP services, that may not be

[44] Financial Action Task Force (2019), *Guidance for a Risk-Based Approach to Trust and Company Service Providers*, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf

supervised for AML/CFT as a TCSP, is necessary and that the AMLSC discuss with the DABs if so.

6.2 Beneficial Ownership

One of the main issues that has been identified in terms of risk is obscurity relating to beneficial ownership. This can be a particular concern in relation to TCSPs with complex clients, those offering nominee services and where a TCSP is providing multiple services.

Article 3(6)(a)(ii) of 4AMLD (transposed into Irish law by section 33 of the CJA 2010 as amended) provides that if, after having exhausted all possible means and provided there are no grounds for suspicion:

- no beneficial owner is identified; or
- if there is any doubt that the person(s) identified are the beneficial owner(s),
  the Register for Beneficial Ownership of Corporate Entities may include the natural person (or persons) who hold the position of senior managing official (or officials). Designated Persons, including TCSPs, are required to keep records of the actions taken in order to identify the beneficial ownership.

It is a concern that the clients of TCSPs may identify senior managing officials as the beneficial owner, with officers of the TCSP who are providing Director services being identified in some cases where it may not be warranted. This should only be used if the TCSP has probed in sufficient detail to discern who the real underlying ultimate beneficial owner is and this has proven impossible.

Recommendation:

It is recommended that supervisors review their TCSP supervisory process in order to ensure that adequate and effective engagement is undertaken with TCSPs to ascertain whether TCSPs can demonstrate adequate understanding of:

(a) their clients;
(b) the nature of the client's business and purpose of the legal structure;
(c) the beneficial owners of their clients; and
(d) the purpose of the transactions they are facilitating.

It is recommended that enforcement action under the CJA 2010 as amended should also be considered by supervisors where the senior management official is recorded as the beneficiary when this is found not to have been warranted.

6.3 Provision of TCSP Services to Complex Legal Entities

As noted above, TCSPs operating in Ireland vary greatly in nature, with some being straightforward and easy to understand, and others dealing with multiple complex legal entities.

Recommendation:

It is recommended that the competent authorities consider the nature of the clients of TCSPs established in this jurisdiction and consider the supervision of those TCSPs and

the adequacy of the skills and resourcing needed to supervise them, in terms of specialist knowledge and complex investigation and enforcement capability.

6.4 Regular meetings of TCSP Supervisors

As noted above, the approach to supervision of TCSPs by competent authorities can vary in practice, while different competent authorities may have divergent understandings of risk, based on the specific TCSPs they supervise.

Recommendation:

It is recommended that the AMLSC propose the establishment of a TCSP supervisory forum that would meet at least twice a year. The forum would bring together the various supervisors of TCSPs to liaise and coordinate on relevant matters, to discuss developments and trends in relation to TCSPs, to discuss emerging risks and supervisory activity and to agree how to take forward any actions that may be considered warranted

6.5 TCSPs supervised by the AMLCU, where the TCSP is established by individual solicitors in law firms

The European Commission's CSR specifically mentioned "the actual risk exposure of professionals involved in the provision of services to companies and trusts". It is important to note the distinction between TCSPs as defined in the CJA 2010 as amended and professionals such as accountants and solicitors who may be providing legal, accounting and/or company services to TCSPs, but who are not TCSPs themselves. The MoU between the AMLCU and the Law Society highlights that the Law Society (which is a self-regulating body) is the supervisor of solicitors where they provide legal/company services to a TCSP, while the AMLCU is the supervisor in relation to a TCSP established as a company.

Recommendation:

It is recommended that the AMLCU and the Law Society meet with a view to ascertaining whether staff of law firms, which have established TCSPs as companies, are also involved in providing legal and/or company services to those TCSPs. If this is the case, they should consider whether the Law Society, as a competent authority in relation to the provision of legal and/or company services to TCSPs, and the AMLCU as a State competent authority of TCSPs established by staff of legal firms as companies, should exchange information in relation to supervision.

.

Annex 1: Schedule 4 of the Criminal Justice Act 2010

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY HIGHER RISK

(1) Customer risk factors:

(*a*) the business relationship is conducted in unusual circumstances;

(*b*) customers that are resident in geographical areas of higher risk as set out in *subparagraph (3)* ;

(*c*) non-resident customers;

(d*)* legal persons or arrangements that are personal asset-holding vehicles;

(e*)* companies that have nominee shareholders or shares in bearer form;

(f*)* businesses that are cash intensive;

(g*)* the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(h*)* the customer is a third country national who applies for residence rights or citizenship in the State in exchange for capital transfers, purchase of property or government bonds or investment in corporate entities in the State.

(2) Product, service, transaction or delivery channel risk factors:

(a*)* private banking;

(b*)* products or transactions that might favour anonymity;

(c*)* non face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in the Electronic Identification Regulation or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;

(d*)* payment received from unknown or unassociated third parties;

(e*)* new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(f*)* transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare or scientific value, as well as ivory and protected species.

(3) Geographical risk factors:

(a*)* countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(b*)* countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c*)* countries subject to sanctions, embargos or similar measures issued by organisations such as, for example, the European Union or the United Nations;

(d*)* countries (or geographical areas) providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Annex 2: Case Studies related to TCSPs

The below case studies have been provided by Ireland's competent authorities for supervising TCSPs. They have been grouped together by theme.

Lack of CDD / understanding of customer business

Example 1:

At a 2018 inspection, 8 trusts were examined who were clients of a TCSP. In most cases, the beneficiaries of the trusts were described as "family members of the settlor" and there was no record of Customer Due Diligence (CDD) on file for them. For one of the trusts, the beneficiaries were listed as "various charities." This was followed up by the AMLCU, upon which the beneficiaries were listed as "Settlor, family members of settlor and business friends." The AMLCU found through open data research that one of these trusts had been referred to in a case before the UK High Court in 2013. The Court's Judgement referred to a particular individual as a settlor of the trust.

This individual in question had not been referenced in the documents provided to the AMLCU neither during the inspection nor during the follow-up. This highlights that the TCSP may not have had sufficient knowledge or understanding of its clients, that the client had not provided the correct information to the TCSP, or that the TCSP was not providing the correct information to the competent authority. This highlights the importance of TCSPs carrying out CDD on beneficial owners and of TCSPs having a good understanding of the customer and their business or they risk potentially being exposed to ML/TF.

Example 2:

A client of a TCSP was found to be a shareholder in a limited company involved in mining that was under investigation in the United States in relation to potential bribery and corruption in Central Africa and Central Asia. It was alleged that the beneficial owner of the mining company had a corrupt relationship with a leader in an Asian country, and that vast wealth had been transferred to the leader at the expense of shareholders of the firm. Other allegations being considered related to potential fraud in an Initial Public Offering (IPO.) This example highlights the importance of CDD and of TCSPs closely examining a customer's beneficial ownership.

Example 3:

It was reported in the media that an individual had formed companies that were subsequently used for criminal purposes internationally. The individual expressed the view that setting up a company was a one-off transaction and he was not responsible for what happened with a company he formed after he passed it to a client. This example underlines the importance of TCSPs understanding that they must carry out full due diligence for company formation and comply with all aspects of the CJA 2010 as amended (knowing the client and the purpose for which the company will be used etc.). During a certain period in the past, this individual operated a TCSP that was under the supervision of the AMLCU, but was subsequently not granted an authorisation.

Example 4:

A client of a TCSP was found on inspection by the AMLCU to be a subsidiary of a large Russian oil company and was identified as being engaged in oil exploration, which is a sanctioned activity. The AMLCU reported this to the competent authority for sanctions. This highlights the importance of TCSPs having a good understanding of their clients and of their clients business.

Complexity of Ownership Structures

Example 5:

At inspection a client of a TCSP was found to have some very complex structures in place. The beneficial owner of the client is a billionaire national from Asia. One such complex structure was based on a partnership.

“X” Trustees (Ireland) Limited, a TCSP, acted on behalf of their client, the Asian billionaire, as the initial limited partner of a proposed partnership. “Y” Corporate Trustees (Mauritius) Limited, a TCSP, expressed an interest in becoming a partner in its role as trustee for “Z” Trust Limited. “Z” Trust Limited is a company limited by shares and incorporated in the British Virgin Islands.

Other countries through which the client did business include Switzerland and the Cayman Islands. The sum of the values of the sampled entities of the client of the TCSP was over half a billion US dollars. The TCSP could not adequately explain the reasons for the complexity of the arrangements.

Rialtas na hÉireann
Government of Ireland

Tithe an Rialtas. Sráid Mhuirfean Uacht,
Baile Átha Cliath 2, D02 R583, Éire
Government Buildings, Upper Merrion Street,
Dublin 2, D02 R583, Ireland

T:+353 1 676 7571
@IRLDeptFinance
www.gov.ie/finance